HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. **200300134-2**

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): **Michael John WRAY et al.**

Confirmation No.: 8275

Application No.: 10/811,305

Examiner: Harris C. WANG

Filing Date: **March 29, 2004**

Group Art Unit: **2439**

Title: SECURITY POLICY IN TRUSTED COMPUTING SYSTEMS

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on March 18, 2009 .

☒ The fee for filing this Appeal Brief is $540.00 (37 CFR 41.20).

□ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

□ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

□ 1st Month $130	□ 2nd Month $490	□ 3rd Month $1110	□ 4th Month $1730

□ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 540 . At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

Michael John WRAY et al

By

Ashok K. Mannava

Attorney/Agent for Applicant(s)

Reg No. : 45,301

Date : May 19, 2009

Telephone : (703) 652-3822

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200300134-2

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Michael John WRAY et al.

Confirmation No.: 8275

Application No.: 10/811,305

Examiner: Harris C. WANG

Filing Date: March 29, 2004

Group Art Unit: 2439

Title: SECURITY POLICY IN TRUSTED COMPUTING SYSTEMS

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on March 18, 2009 .

☒ The fee for filing this Appeal Brief is $540.00 (37 CFR 41.20).

□ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

□ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

□ 1st Month $130 □ 2nd Month $490 □ 3rd Month $1110 □ 4th Month $1730

□ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 540 . At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

Michael John WRAY et al.

By Ashok M

Ashok K. Mannava

Attorney/Agent for Applicant(s)

Reg No. : 45,301

Date : May 19, 2009

Telephone : (703) 652-3822

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Attorney Docket No.: 200300134-2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Michael John WRAY et al.	**Confirmation No.:**	8275
Serial No.:	10/811,305	**Examiner:**	Harris C. WANG
Filed:	March 29, 2004	**Group Art Unit:**	2439

Title: SECURITY POLICY IN TRUSTED COMPUTING SYSTEMS

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF - PATENTS

Sir:

This is an Appeal Brief in connection with the decisions of the Examiner in a Final Office Action dated January 16, 2009. Each of the topics required in an Appeal Brief and a Table of Contents are presented herewith and labeled appropriately.

TABLE OF CONTENTS

(1) Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, L.P.

(2) Related Appeals and Interferences

There are no other appeals or interferences related to this case.

(3) Status of Claims

Claims 1-12 are pending in the present application of which claims 1 and 12 are independent. Claims 1-12 are all rejected and are all appealed.

(4) Status of Amendments

No amendment was filed subsequent to the final Office Action dated January 16, 2009.

(5) Summary of Claimed Subject Matter

Independent claims 1 and 12 and dependent claims 2 and 4 are the claims that are argued in this appeal. It should be understood that the citations below to the original disclosure as providing support for the claimed features are merely exemplary and do not limit the claimed features to only those citations. Thus, other sections in the present application may provide the same or additional supports as well.

1. A system comprising a trusted computing platform including:

at least one first logically protected computing compartment associated with initialization of said system (see modules 15 of Fig. 1; page 6, lines 2-4; and page 9, lines 4-5), and

at least one second logically protected computing compartment, each second logically protected computing compartment being associated with at least one service or process supported by said system (see modules 15 of Fig. 1; page 6, lines 2-4; and from page 6, line 28 to page 7, line 19),

wherein the system is arranged to load onto said trusted computing platform a predetermined security policy including at least one security rule for controlling the operation of each of said logically protected computing compartments (see page 7, lines 7-19);

wherein the security rule relating to the at least one first logically protected computing compartment is arranged to be loaded onto said trusted computing platform when the system is initialized (see steps 110 to 120 of Fig. 4A; from page 8, line 26 to page 9, line 5; and page 9, lines 26-27), and

wherein the at least one security rule relating to the at least one second logically protected computing compartment is only arranged to be loaded onto said trusted computing platform if one or more services or processes associated therewith are enabled (see steps 124 to 138 of Fig. 4B; and page 9, lines 7-13 and 27-28).

2. A system according to claim 1, wherein one or more common variable is defined for each compartment, wherein a relevant security rule is only arranged to be added if

the variable associated with a particular compartment is enabled (see page 4, lines 18-26; page 9, lines 10-13; and page 10, lines 10-11).

4. A system according to claim 3, wherein the system is arranged to determine, in response to a compartment being enabled, a status of said at least one variable and cause a relevant plug-in based upon the directory of plug-ins to run only if an associated variable is 'true' (see page 4, lines 18-26; page 9, lines 10-13).

12. A method of loading a security policy onto a system including a trusted computing platform, said trusted computing platform including at least one first logically protected computing compartments associated with initialization of said system (see modules 15 of Fig. 1; page 6, lines 2-4; and page 9, lines 4-5), and at least one second logically protected computing compartments, the at least one second logically protected computing compartments being associated with at least one service or process supported by said system (see modules 15 of Fig. 1; page 6, lines 2-4; and from page 6, line 28 to page 7, line 19), said security policy comprising one or more security rules for controlling the operation of said the at least one logically protected computing compartments (see page 7, lines 7-19), the method including the steps of:

loading said security rules relating to the at least one first logically protected computing compartments onto said trusted computing platform when the system is initialized (see steps 110 to 120 of Fig. 4A; from page 8, line 26 to page 9, line 5; and page 9, lines 26-27), and loading the at least one security rule relating to the at least one second logically protected computing compartments onto said trusted computing platform only if one or more services or processes associated therewith are enabled (see steps 124 to 138 of Fig. 4B; and page 9, lines 7-13 and 27-28).

(6) Grounds of Rejection to be Reviewed on Appeal

A. Whether claims 1-2 and 10-12 were properly rejected as being anticipated under 35 U.S.C. § 102(b) by U.S. Patent Application Publication No. 2002/0194496 to Griffin et al. (hereinafter "Griffin").

B. Whether claims 3-9 were properly rejected under 35 U.S.C. §103(a) as being unpatentable over Griffin in view of U.S. Patent Application Publication No. 2004/0003288 to Wiseman et al. (hereinafter "Wiseman").

(7) Arguments

A. The rejection of claims 1-2 and 10-12 under 35 U.S.C. § 102(b) as being anticipated by Griffin should be reversed

The test for determining if a reference anticipates a claim, for purposes of a rejection under 35 U.S.C. § 102, is whether the reference discloses all the elements of the claimed combination, or the mechanical equivalents thereof functioning in substantially the same way to produce substantially the same results. As noted by the Court of Appeals for the Federal Circuit in *Lindemann Maschinenfabrick GmbH v. American Hoist and Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984), in evaluating the sufficiency of an anticipation rejection under 35 U.S.C. § 102, the Court stated:

> Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim.

Therefore, if the cited reference does not disclose each and every element of the claimed invention, then the cited reference fails to anticipate the claimed invention and, thus, the claimed invention is distinguishable over the cited reference.

In the Office Action, claims 1-2 and 10-12 were rejected under 35 U.S.C. § 102(b) as being anticipated by Griffin. The rejection should be reversed for the following reasons.

- Independent claim 1:

Independent claim 1 recites:

> wherein the security rule relating to the at least one first logically protected computing compartment is arranged to be loaded onto said trusted computing platform when the system is initialized, and
>
> wherein the at least one security rule relating to the at least one second logically protected computing compartment is only arranged to be loaded onto said trusted computing platform if one or more services or processes associated therewith are enabled.

More simply, claim 1 recites different timings for loading security rules: (1) the security rule for the first compartment is arranged to be loaded when the system is initialized, and (2) the security rule for the second compartment is arranged to be loaded only when the services or processes associated with the second compartment are enabled. Such a difference in the timing and conditions for loading the security rules is the difference between the prior art and the present invention, as clearly described in the present application. More specifically, the present application discloses that, in the prior art, the security rules for all of the computing compartments are loaded at the initialization of the system, irrespective of whether any of the services associated with those compartments are enabled (see the present application, page 2, lines 17-21 and page 8, lines 15-18). The present application also discloses that such a loading at the initialization of the system in the prior art is not efficient, convenient or practical for the system (see from page 2, line 22 to page 3, line 9). In contrast, in the present claimed invention, the security rule for the first compartment is loaded at the initialization of the system, but the security rule for the second compartment is loaded only if the services or processes associated with the second compartment are enabled. In other words, in the claimed invention, if the services or processes associated with the second compartment are not enabled, the security rule for the second compartment would not be loaded.

Griffin fails to teach or suggest the above recited features of claim 1. Griffin discloses in Fig. 1 a computing platform 20 having a trusted device 213 and a plurality of computing compartments 24, wherein the trusted device 213 performs a secure boot process when the computing platform 20 is reset (see paragraph [0025]). Furthermore, Griffin discloses that the computing compartments 24 are loaded with security rules to ensure that resources from one compartment cannot interfere with resources from another compartment (see paragraphs [0033] and [0036]). However, Griffin does not disclose when the security rules are loaded for the compartments 24. In fact, Griffin does not mention the timing and conditions for the loading of the security rules. It appears that, in Griffin, the security rules are always present for the compartments. At best, the security rules in Griffin are loaded at the time the computing platform 20 is reset (paragraph [0025]), but not at different times when the services or processes are enabled, as recited in claim 1. As a result, Griffin fails to teach the different timings for loading security rules for computing compartments 24.

Griffin, thus, fails to teach or suggest "the at least one security rule relating to the at least one second logically protected computing compartment is only arranged to be loaded onto said trusted computing platform if one or more services or processes associated therewith are enabled," as recited in claim 1.

In the rejection of claim 1, the Examiner asserts that Griffin discloses the claimed feature of "the at least one security rule relating to the at least one second logically protected computing compartment is only arranged to be loaded onto said trusted computing platform if one or more services or processes associated therewith are enabled" in paragraphs [0036] and [0068]. However, such an assertion is respectfully traversed because paragraphs [0036] and [0068] do not disclose that feature. In paragraph [0036], Griffin describes the nature of the security rules, which is for controlling the communication between compartments. Paragraph [0036] does not disclose when the security rules are to be loaded, as recited in claim 1. In paragraph [0068], Griffin discloses that the computing environments 24 in Fig. 1 can be subdivided so that multiple applications can be run on the guest operating system 25. Such a disclosure in paragraph [0068] has nothing related to when the security rules are arranged to be loaded for the compartments. In particular, Griffin fails to teach that a security rule for an application is loaded only if the service for the application is enabled.

Therefore, paragraphs [0036] and [0068] fails to teach the security rule relating to the second computing compartment is only arranged to be loaded if the services or processes associated with the second compartment are enabled, as proposed by the Examiner.

At least for the reasons set forth above, it is respectfully submitted that independent claim 1 is patentable over Griffin because Griffin fails to teach all of the features recited in claim 1. Therefore, reversal of the rejection and allowance of independent claim 1 is respectfully requested.

- Independent Claim 12:

Claim 12 recites:

> loading said security rules relating to the at least one first logically protected computing compartments onto said trusted computing platform when the system is initialized, and
>
> loading the at least one security rule relating to the at least one second logically protected computing compartments onto said trusted computing platform only if one or more services or processes associated therewith are enabled.

The above features are similar to the features recited in claim 1 above. Therefore, claim 12 is believed to allowable over Griffin for at least the same reasons set forth above with respect to independent claim 1. Thus, reversal of the rejection and allowance of independent claim 12 is respectfully requested.

- Dependent Claims 2, 10 and 11:

Claims 2, 10 and 11 are dependent from allowable independent claim 1. Therefore, these claims are also believed to be allowable over the cited documents of record for at least the same reasons set forth above with respect to independent claim 1.

Moreover, dependent claims 2, 10 and 11 recite additional features not found in the cited documents of record, including Griffin. For instance, claim 2 recites that a relevant security rule for a compartment is only arranged to be added if a common variable for that particular compartment is enabled. Griffin fails to disclose such a feature. In the rejection of claim 2, the Examiner quotes a description in paragraph [0034] of Griffin to imply that

Griffin discloses the feature of claim 2. However, paragraph [0034] of Griffin does not mention any variables for a compartment, much less the condition that a security rule for the compartment is only arranged to be added if the variable for that compartment is enabled. Rather, paragraph [0034] of Griffin teaches that each resource is given a label to indicate that the resource belongs to a compartment, and that the kernel of the host operating system controls the access of the resources such that the resources from one compartment do not interfere with the resources from another compartment. Such a description in paragraph [0034] of Griffin fails to teach the condition of when a security rule for a compartment is added for a compartment, as recited in claim 2. Even if somehow the Examiner equates the resources for a compartment to the configuration variables recited in claim 2, Griffin still fails to teach the condition that the security rule is only arranged to be added if the resources are enabled. Thus, Griffin fails to teach the feature recited in claim 2.

In view of the foregoing discussions, reversal of the rejection and allowance of claims 2, 10 and 11 are respectfully requested.

B. The rejection of claims 3-9 under 35 U.S.C. §103(a) as being unpatentable over Griffin in view of Wiseman should be reversed

The test for determining if a claim is rendered obvious by one or more references for purposes of a rejection under 35 U.S.C. § 103 is set forth in *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007):

> "Under §103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter

> sought to be patented." Quoting *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1 (1966).

As set forth in MPEP 2143.03, to ascertain the differences between the prior art and the claims at issue, "[a]ll claim limitations must be considered" because "all words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385. According to the Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in view of *KSR International Co. v. Teleflex Inc.*, Federal Register, Vol. 72, No. 195, 57526, 57529 (October 10, 2007), once the *Graham* factual inquiries are resolved, there must be a determination of whether the claimed invention would have been obvious to one of ordinary skill in the art based on any one of the following proper rationales:

> (A) Combining prior art elements according to known methods to yield predictable results; (B) Simple substitution of one known element for another to obtain predictable results; (C) Use of known technique to improve similar devices (methods, or products) in the same way; (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (E) ''Obvious to try''—choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention. *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007).

Furthermore, as set forth in *KSR International Co. v. Teleflex Inc.*, quoting from *In re Kahn*, 441 F. 3d 977, 988 (CA Fed. 2006), "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasonings with some rational underpinning to support the legal conclusion of obviousness."

Therefore, if the above-identified criteria and rationales are not met, then the cited reference(s) fails to render obvious the claimed invention and, thus, the claimed invention is distinguishable over the cited reference(s).

Claims **3-9** were rejected under 35 U.S.C. §103(a) as being unpatentable over Griffin in view of Wiseman. The rejection should be reversed for the following reasons.

As discussed above with respect to independent claim 1, from which claims 3-9 depend, Griffin fails to disclose all of the features of independent claim 1. In setting forth the rejection of claims 3-9, the Examiner has not and cannot reasonably assert that the disclosure contained in Wiseman makes up for any of the deficiencies discussed above with respect to Griffin. Accordingly, even assuming for the sake of argument that one of ordinary skill in the art were somehow motivated to modify Griffin with the disclosure contained in Wiseman, the proposed modification would still fail to yield all of the features of independent claim 1.

Moreover, claims 3-9 recite additional features not found in the cited documents of record, including Griffin and Wiseman. For instance, claim 4 recites that the system is arranged to cause a relevant plug-in to run only if an associated variable is true. Griffin fails to teach such a feature. In the rejection of claim 4, the Examiner refers to paragraph [0032] of Griffin, which states that the compartment is controlled by a kernel of the host operating system. However, the statement that the kernel controls the compartment in paragraph [0032] of Griffin fails to particularly teach or suggest that a plug-in is controlled to run only if a variable associated with the compartment is true. Thus, Griffin fails to teach the feature of claim 4. Wiseman also fails to mention any plug-ins being operated when a variable is true. Therefore, Griffin and Wiseman, taken individually or in combination, fail teach that the system is arranged to cause a relevant plug-in to run only if an associated variable is true.

For at least the foregoing reasons, the Examiner has failed to establish that claims 3-9 are prima facie obvious in view of the combined disclosures contained in Griffin and Wiseman as proposed in the Office Action. Therefore, reversal of the rejection and allowance of claims 3-9 are respectfully requested.

(8) Conclusion

For at least the reasons given above, the rejections of claims 1-12 are improper. Accordingly, it is respectfully requested that such rejections by the Examiner be reversed and these claims be allowed. Attached below for the Board's convenience is an Appendix of claims 1-12 as currently pending.

Please grant any required extensions of time and charge any fees due in connection with this Appeal Brief to deposit account no. 08-2025.

Respectfully submitted,

Dated: May 19, 2009

By

Ashok K. Mannava
Registration No.: 45,301

MANNAVA & KANG, P.C.
11240 Waples Mill Road
Suite 300
Fairfax, VA 22030
(703) 652-3819 (or 3822)
(703) 865-5150 (facsimile)

(9) Claim Appendix

1. (Previously Presented) A system comprising a trusted computing platform including:

at least one first logically protected computing compartment associated with initialization of said system, and

at least one second logically protected computing compartment, each second logically protected computing compartment being associated with at least one service or process supported by said system,

wherein the system is arranged to load onto said trusted computing platform a predetermined security policy including at least one security rule for controlling the operation of each of said logically protected computing compartments;

wherein the security rule relating to the at least one first logically protected computing compartment is arranged to be loaded onto said trusted computing platform when the system is initialized, and

wherein the at least one security rule relating to the at least one second logically protected computing compartment is only arranged to be loaded onto said trusted computing platform if one or more services or processes associated therewith are enabled.

2. (Previously Presented) A system according to claim 1, wherein one or more common variable is defined for each compartment, wherein a relevant security rule is only arranged to be added if the variable associated with a particular compartment is enabled.

3. (Previously Presented) A system according to claim 2, wherein at least one variable associated with a directory of plug-ins is arranged to be added.

4. (Previously Presented) A system according to claim 3, wherein the system is arranged to determine, in response to a compartment being enabled, a status of said at least one variable and cause a relevant plug-in based upon the directory of plug-ins to run only if an associated variable is 'true'.

5. (Previously Presented) A system according to claim 4, wherein the at least one compartment includes an operating system compartment arranged to be controlled by the operating system kernel.

6. (Previously Presented) A system according to claim 5, wherein the at least one compartment and network resources are arranged so communication between them is provided via relatively narrow kernel level controlled interfaces to a transport mechanism.

7. (Previously Presented) A system according to claim 6, wherein said communication is governed by rules specified on a compartment by compartment basis.

8. (Previously Presented) A system according to claim 7, including means for determining when a service is starting, and on being enabled, for loading the compartment associated with that service and loading the at least one security rule associated with that service.

9. (Previously Presented) A system according to claim 8, including means for determining when a service starts, and causing the at least one security rule to be loaded accordingly.

10. (Previously Presented) A system according to claim 1, wherein the at least one compartment includes an operating system compartment arranged to be controlled by the operating system kernel.

11. (Original) A system according to claim 1, including means for determining when a service is starting, and on being enabled, for loading the compartment associated with that service and loading the security rules associated with that service.

12. (Previously Presented) A method of loading a security policy onto a system including a trusted computing platform, said trusted computing platform including at least one first logically protected computing compartments associated with initialization of said system, and at least one second logically protected computing compartments, the at least one second logically protected computing compartments being associated with at least one service or process supported by said system, said security policy comprising one or more security rules for controlling the operation of said the at least one logically protected computing compartments, the method including the steps of:

loading said security rules relating to the at least one first logically protected computing compartments onto said trusted computing platform when the system is initialized, and loading the at least one security rule relating to the at least one second logically protected computing compartments onto said trusted computing platform only if one or more services or processes associated therewith are enabled.

(10) Evidence Appendix

None.

(11) Related Proceedings Appendix

None.